Enterprise Information Security Charter [1]

Topics:
security policy [2], authority [3], charter [4], framework [5], GTA review [6], security framework [7]

PS-08-005 Enterprise Information Security Charter

Issue Date: 3/20/2008

Revision Effective Date: 3/20/2008

PURPOSE

The state of Georgia is committed to protecting the information assets of the state and its constituents. All state agencies have a responsibility of due diligence and due care to that commitment. This policy reinforces that GTA is the authority to set statewide security governance and establishes the requirement for each agency to develop and maintain an internal information security program that adequately and effectively protects the information assets, personnel and facilities under their control based on an assessment of risks and business objectives.

Information security policies raise awareness of users to the potential risks associated with information technology. Employee awareness through dissemination of the policies helps minimize the cost of security incidents, accelerate the development of new application systems, and assure the consistent implementation of controls for information systems throughout the organization.

State of Georgia data is a valuable asset that must be protected. Prudent steps must be taken to ensure that its integrity, confidentiality, and availability are not compromised. This policy demonstrates the commitment of the State and establishes the requirement to create, maintain, and adhere to a uniform set of information security policies, standards and general guidelines.

SCOPE

All State Agencies, as defined in the Official Code of Georgia Annotated § 50-25-1(b)(1) and all users (employees, contractors, vendors, and other parties) of State of Georgia information technology resources are expected to understand and abide by them.

POLICY

The State of Georgia, through the authority granted to the Georgia Technology Authority (GTA), shall create a framework of policies, standards and practices to facilitate an information security infrastructure based on the risk management framework established by the Federal Information Security Management Act (FISMA) of 2002 and the supporting documentation developed by the National Institute of Standards (NIST), that protects the integrity, confidentiality, and availability of its information assets from unauthorized disclosure, modification, use, or destruction, while still meeting business objectives.

The GTA Office of Information Security (OIS) shall development Enterprise security policies and standards that: identify and address general areas of risk; are clear, concise, measurable, and verifiable; provide a basis for compliance audits; and balance protection with productivity. OIS shall conduct periodic reviews of policies and standards to assess their effectiveness and issue updates as necessary.

All Agencies that create, use or maintain information assets for the State of Georgia shall develop, document, implement, and maintain an internal information security infrastructure that establishes a security management organization, that assesses risk, that develops and implements policies, processes, and technology to adequately protect the information assets, personnel and facilities under their control; and ensuring compliance with Enterprise policies and standards and federal and state requirements such as but not limited to HIPAA, FERPA, COPPA, GLBA and CJIS.

TECHNOLOGY SECURITY AUTHORITY

GTA is authorized by law to ?establish technology security standards and services to be used by all agencies[1]?. Official Code of Georgia Annotated (O.C.G.A.) § 50-25-4(a)(21) (2007). These standards and services flow from the technology security policies adopted by the GTA Board and shall be adhered to by all agencies that have not followed the exemption procedure.[2]

This authority in the area of security is broader than the general statutory authority granted GTA with respect to technology policies. O.C.G.A. § 50-25-4(a)(10) vests GTA with the authority to ?set technology policy for all agencies[1] except those under the authority, direction, or control of the General Assembly or state wide elected officials other than the Governor.?

Statewide security standards and the policies that underlay them are binding upon all agencies except agencies within the judicial branch, institutions under and including the Georgia Board of Regents, and the Superior Court Clerks Cooperative Authority. These exempt entities have the discretion to adopt a GTA security standard or policy, modify it as it pertains to the exempt agency, or follow another policy. GTA invites discussion with exempt entities when questions arise.

[1] Agency is defined as ?every state department, agency, board, bureau, commission, and authority which shall not include any agency within the judicial branch of state government or the University System of Georgia and shall also not include any authority statutorily required to effectuate the provisions of Part 4 of Article 9 of Title 11.? O.C.G.A. § 50-25-1(b)(1) (2006).

[2] The scope of certain Policies may only apply to certain agencies that are within a ?common community of interest.? An example may be certain Policies dealing with HIPAA related data may only apply to agencies that handle certain patient or medical data. The same may be true for certain Standards or Guidelines.

ENFORCEMENT

The State of Georgia enterprise information security policies and standards are based upon the Federal Information Security Management Act (FISMA) and ISO 27000 series standard of best practices. Individual state agencies are responsible for developing internal policies and procedures to facilitate compliance with these enterprise security policies and standards. While these policies and standards are designed to comply with or compliment federal and state laws and regulations; if there is a conflict, those applicable laws and regulations will take precedence agencies shall implement whatever procedures are necessary to comply.

Violations of policy could result in serious security incidents involving sensitive state or federal data. Violators may be subject to disciplinary actions which may include termination and/or criminal prosecution.

Agencies may impose additional sanctions upon their employees for violations of policies.

The policies and standards will guide periodic security reviews, as well as audits by the State Department of Audits and Accounts (DOAA).

EXCEPTIONS

Exceptions to a policy or standard must be approved by the State Chief Information Officer (CIO) with review by the State Chief Information Security Officer. In each case, the agency or vendor must include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the management approval. Denials of requests for exceptions may be appealed to the State Chief Information Officer. See provisions for submitting an Exemption Request.

REFERENCES

Refer to the following NIST publication for an introduction to Computer Security:

- NIST Pub 800-12 Introduction to Computer Security (NIST Handbook) *http://csrc.nist.gov* *[8]*

RELATED ENTERPRISE POLICIES, STANDARDS, GUIDELINES

Information Security Management Organization (SS-08-006) [9]

Information Security Infrastructure (SS-08-005) [10]

TERMS and DEFINITIONS

Confidentiality - ?Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information?? [44 U.S.C., Sec. 3542]

- A loss of *confidentiality* is the unauthorized disclosure of information.

Integrity - ?Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity?? [44 U.S.C., Sec. 3542]

- A loss of *integrity* is the unauthorized modification or destruction of information.

Availability - ?Ensuring timely and reliable access to and use of information?? [44 U.S.C., SEC. 3542]

- A loss of *availability* is the disruption of access to or use of information or an information system.

Information Security Infrastructure ? the interconnected elements (people, policies, processes, procedures and technology), that provide the framework to support an organizations security philosophy regarding their assets and effectively meeting their business objectives.

Due Diligence and Due Care - the degree of effort and care that a prudent person might be expected to exercise in the examination and evaluation of risks affecting a business transaction.
